

Oracle about to issue 52 new critical patch updates – But application weaknesses are where the serious dangers lie

Database security persists as IT's biggest problem

12 January 2007, Oxford – Oracle has just issued its first ever pre-release announcement flagging up no fewer than 52 new critical patch updates which will be formally issued this Tuesday.

“This is another step in the right direction by Oracle. As ever forewarned is forearmed – and this move allows IT managers to get to grips earlier with essential patching.” says Paul Davie, Secerno CEO. “But users need to beware: it’s not the vendor vulnerabilities they need to focus on but the critical weaknesses in their development processes.”

As more and more companies rely upon databases to support mission critical business activity the importance of database security is growing fast. Vulnerabilities in vendor solutions are an issue and can be mitigated to some extent by timely patching – but users cannot rely on patch management to solve their database security problems. The continuous pressure on developers to drag more and more functionality out of their database should be a much greater cause for concern. Deployment errors caused by poorly configured databases, inappropriate access permissions or badly engineered applications accessing the database are an increasingly worrying trend.

Badly written web applications are a key cause for concern and are responsible for more than 60% of attacks. On demand vulnerability player, Qualys, quotes 100 new issues per week. As Rohit Dhamankar reflected in his presentation at the SANS Top 20 2006 launch, “applications are really written badly ... really badly”; The holes have always been there, but now they are being discovered as more people are looking and automated methods are deployed to find them.

SQL injection - the most serious type of attack affecting databases right now – rising at an alarming rate of 250% year on year growth (according to Mitre¹) – has nothing at all to do with exploiting database vendor vulnerabilities. It’s incorrect filtering of SQL queries that allows an attacker to make his targeted strike on the database.

“Blindsighting” is an increasingly worrying trend. A DBA inherits a database and takes responsibility for managing and upgrading it, without concise and clear knowledge of its abilities, its strengths and its weaknesses.

So what steps can business take now to manage database security? The burning question is “Who is asking the database to do what?”

Clearly organizations need to tighten up their security policy. But they also need to be ahead of the game with a system that effectively isolates each and every request made to the database that is inconsistent with what should normally be going on and prevents the database ever being asked to do something that they really would prefer it didn’t do – even if the request is coming from an authorized source.

Unique new technology developed by data assurance company Secerno uses machine learning algorithms to allow users to build up a rich understanding of application-to-database behaviour and to insist on database interactions conforming only to allowable behaviours. It represents the world’s first database application assurance platform. This approach is not constrained by the usual black list/white list approach which prevents traditional tools from dealing effectively with previously-unseen Zero Day attacks or specifically crafted SQL injections. Along with intrusion detection and prevention, Secerno also provides a number of proactive capabilities which help prevent database attacks, including:

- Determining true least privilege access to the database, by monitoring the questions being asked of it – foiling attacks seen or unseen, from within or outside the organisation
- Creating an efficient, targeted, secure log, to supporting audit and compliance
- Automatically highlighting how engineering quality can be improved in applications accessing critical data

¹ See http://www.darkreading.com/document.asp?doc_id=103774&WT.svl=news1_1

- automatically identifying dormant software features for future removal

To speak to Paul Davie, Secerno CEO, about these burning issues or for more information, please get in touch with Jane Folwell via 01344 845132 or 07950 033370.

www.secerno.com

For Oracle pre-release see <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html>